UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

BRADLEY COOPER, on behalf of himself and all others similarly situated, *Plaintiff*, v. BONOBOS, INC., *Defendant.*	Case No. 1:21-cv-854-JMF **AMENDED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

AMENDED CLASS ACTION COMPLAINT

Plaintiff Bradley Cooper ("Plaintiff"), individually and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to himself and on information and belief as to all other matters, by and through undersigned counsel, hereby files this Amended Class Action Complaint against Defendant Bonobos, Inc. ("Defendant," "Bonobos," or the "Company").

I. NATURE OF THE ACTION

1. Hackers infiltrated and accessed the Company's inadequately protected cloud backup database in or about August 2020. During that time, the hackers who are "threat actors"[1] known as Shiny Hunters and notorious for hacking online services and selling stolen databases, stole the protected personal information of some or all of Bonobos' seven million customers who shopped at the Company's website ("Private Information") and then posted the stolen information to a hacker website forum. The leaked database included a "70 GB SQL file" containing various internal tables used by Bonobos. The database reportedly included customers' addresses, phone numbers, partial

[1] A "threat actor," also called a malicious actor or bad actor, is an entity that is partially or wholly responsible for an incident that impacts – or has the potential to impact – an organization's security. https://whatis.techtarget.com/definition/threat-actor (last accessed April 14, 2021).

credit card numbers (including the last four digits), order information, and password histories, as well as customer email addresses, and IP addresses (the "Data Breach").[2]

2. On information and belief, the threat actors also turned the cracked passwords into a list used in credential stuffing attacks, which involves utilizing the log in information using the stolen credentials to access other websites.[3]

3. After being contacted by industry specialists, Bonobos claimed that the threat actors did not gain access to internal systems, but rather, to a backup file hosted in an external cloud environment. According to news reports, Bonobos stated:

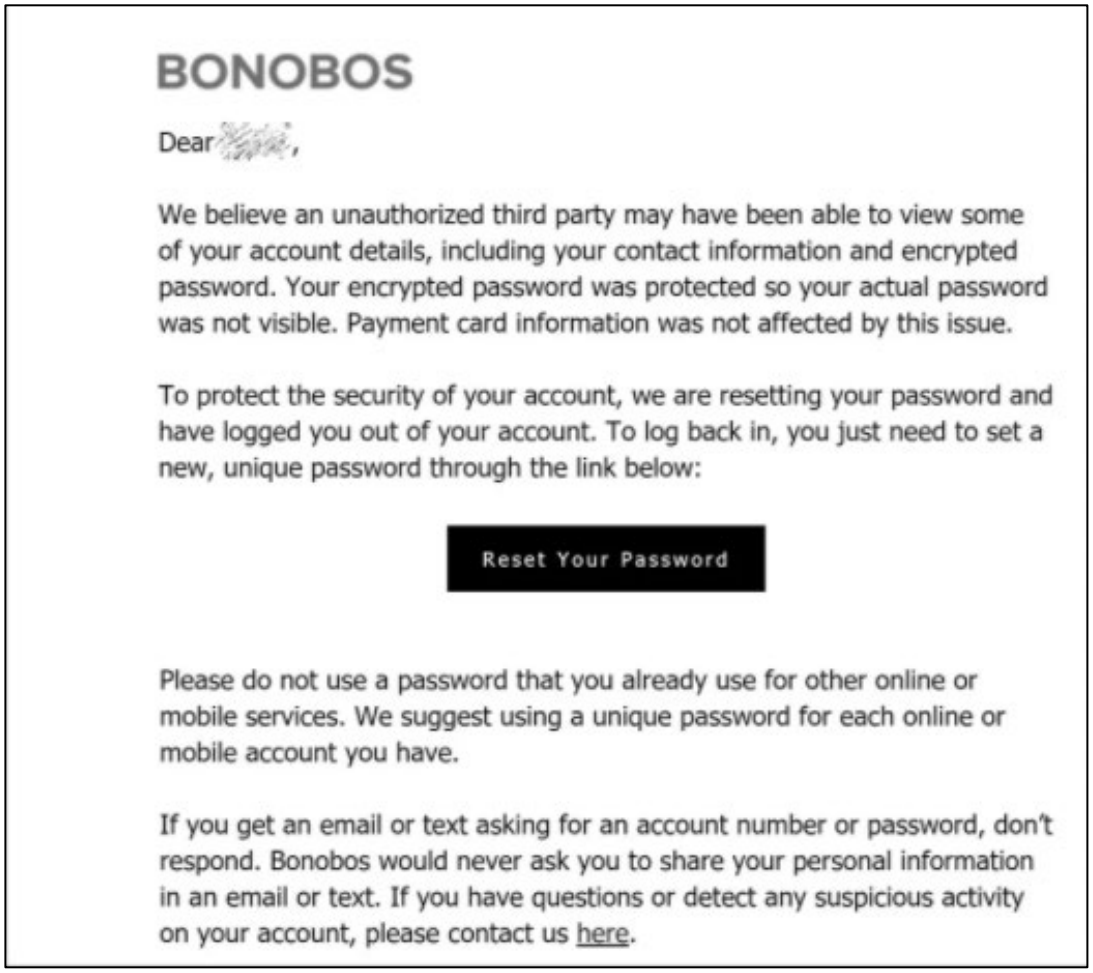
> Protecting our customers' data is something we take very seriously. We're investigating this matter further and, so far, have found no evidence of unauthorized parties gaining access to Bonobos' internal system. What we have discovered is an unauthorized third party was able to view a backup file hosted in an external cloud environment. We contacted the host provider to resolve this issue as soon as we became aware of it. …
>
> Also, we have taken additional precautionary steps, including turning off access points, invalidating account passwords and requiring password resets, to further secure customer accounts. We're emailing customers to notify them that their contact information and encrypted passwords may have been viewed by an unauthorized third party. Payment information was not affected by this issue.[4]

[2] "Bonobos clothing store suffers a data breach, hacker leaks 70GB database," BleepingComputer, https://www.bleepingcomputer.com/news/security/bonobos-clothing-store-suffers-a-data-breach-hacker-leaks-70gb-database/ (last accessed April 14, 2021).

[3] Credential stuffing is the automated injection of breached username/password pairs in order to fraudulently gain access to user accounts. This is a subset of the brute force attack category: large numbers of spilled credentials are automatically entered into the websites until they are potentially matched to an existing account, which the attacker can then hijack for their own purposes. *See Credential Stuffing*, https://owasp.org/www-community/attacks/Credential_stuffing (last accessed April 14, 2021).

[4] "Bonobos Suffers Huge Data Breach," BleepingComputer, https://risnews.com/bonobos-suffers-huge-data-breach (last accessed April 14, 2021).

4. On or about January 22, 2021, Bonobos began emailing breach notifications to affected customers, with the following email message:



BONOBOS

Dear [redacted],

We believe an unauthorized third party may have been able to view some of your account details, including your contact information and encrypted password. Your encrypted password was protected so your actual password was not visible. Payment card information was not affected by this issue.

To protect the security of your account, we are resetting your password and have logged you out of your account. To log back in, you just need to set a new, unique password through the link below:

Reset Your Password

Please do not use a password that you already use for other online or mobile services. We suggest using a unique password for each online or mobile account you have.

If you get an email or text asking for an account number or password, don't respond. Bonobos would never ask you to share your personal information in an email or text. If you have questions or detect any suspicious activity on your account, please contact us here.

5. On information and belief, Plaintiff's and Class members' Private Information was stolen by threat actors. Plaintiff's and Class members' Private Information can be used for criminal purposes, such as fraudulent text messaging schemes, email scams, identity theft and fraudulent purchases -- including phishing, which is a criminal attack performed by cybercriminals to obtain sensitive information such as online passwords, by impersonating a reliable entity in a digital text or email communication -- and may be sold by the threat actors responsible for the Data Breach to other criminals on the dark web.

6. Defendant's conduct – failing to take adequate and reasonable measures to ensure that its customer data was protected, failing to take available steps to prevent and stop the breach,

failing to take adequate measures to detect the breach, failing to provide timely notice of the Data Breach so that five months had passed before providing its customers with notice of the breach, and enabling the threat actors to execute the Data Breach and steal Plaintiff's and Class members' Private Information – has caused substantial harm and injuries to consumers across the country.

7. Defendant Bonobos' material failures put Plaintiff's and Class members' Private Information and interests at serious, immediate, and ongoing risk and, additionally, caused costs and expenses to Plaintiff and Class members associated with time and money spent as a result of taking time and incurring costs to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach.

II. JURISDICTION AND VENUE

8. This Court has diversity jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 class members, the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and many members of the class are citizens of states different from Defendant.

9. The Court has personal jurisdiction over Defendant because Defendant maintains its headquarters in New York, regularly conducts business in New York, and has sufficient minimum contacts in New York. Further, Defendant's officers direct, control and coordinate Bonobos' actions from New York.

10. Venue is proper in this District under 28 U.S.C. § 1391(b)(1) because Defendant maintains its principal place of business in this District and therefore resides in this District pursuant to 28 U.S.C. § 1391(c)(2).

III. PARTIES

Plaintiff

11. Plaintiff Bradley Cooper is a citizen of the State of New York. Mr. Cooper received

an email from Bonobos on or about January 22, 2021 informing him of the Data Breach. Mr. Cooper began receiving a material increase in suspicious text messages and emails after the Bonobos Data Breach. As a result of the Data Breach, Mr. Cooper is compelled to more carefully monitor his emails, text messages, and mobile phone calls, as well as his credit card statements and other accounts. Mr. Cooper has purchased spam text and mobile phone call blocking protection for his mobile device at a cost of $19.99 per year and credit repair and identity theft protection at a cost of $85 per month. In addition, Plaintiff Cooper also froze his credit at a national credit reporting bureau, as alleged herein.

12. Plaintiff suffered actual injury in the form of monetary damages to and diminution in the value of his Private Information, a form of intangible property that he entrusted to Defendant for the purpose of making online purchases, which Private Information was compromised as a result of the Data Breach. Additionally, Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of future fraud and identity theft and misuse posed by his Private Information being placed in the hands of criminals. In addition, Plaintiff suffered actual damages because he spent money on spam text and identity theft protection and spent many hours of his time that he will never get back, addressing the data breach.

13. Like Plaintiff Cooper, other Class members have a continuing interest in ensuring that their Private Information is protected and safeguarded from future breaches.

14. The injuries suffered by Plaintiff and Class members as a direct result of the Data Breach include one or more of the following:

a. unauthorized use of their Private Information;

b. theft of their Private Information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their Private Information;

d. damages arising from the inability to use their Private Information;

e. Time spent and costs associated with the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, including a material increase in spam texts, phone calls, and emails, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach;

f. damages to and diminution in value of their Private Information entrusted to Defendant for the purpose of purchasing products and services from websites operated by Defendant; and

g. the loss of Plaintiff's and Class members' privacy.

Defendant

15. Defendant Bonobos is a Delaware corporation with its principal place of business in New York, New York that operates an online men's clothing store serving customers throughout the United States, as well as approximately sixty physical locations.

16. Defendant Bonobos makes sizeable profits at the expense of its loyal customers; however, Bonobos betrayed the trust of its customers by putting their Private Information at risk of attack by cybercriminals. Bonobos' actions and/or inaction exposed its customers' Private Information, including highly sensitive Private Information, to cyberattack. Through this lawsuit, the numerous affected consumers who entrusted their Private Information to Bonobos have a voice in Plaintiff Cooper.

17. Defendant Bonobos began as an upscale online men's clothing store in or about 2007, which later expanded to approximately sixty physical locations. In or about 2017, Walmart purchased Bonobos for $310 million to offer Bonobos' clothing on Walmart's Jet.com website. Thereafter, Bonobos' online business and presence has significantly expanded through the present.

18. To make purchases through Bonobos, customers must enter their name, billing address, shipping address, email, and payment card information, among other personal details.

IV. STATEMENT OF FACTS

The Data Breach

19. Bonobos was strictly an online business for the first four years of its business, which launched in or about 2007. The Company is popular with male shoppers who dislike shopping for clothing in physical stores.

20. The Company's customer service team – known as Ninjas -- are contacted by customers through email, phone, and video chat. Bonobos uses its social media to request customer feedback on design ideas.

21. Bonobos' website Privacy Policy states that the Company collects the following personal information about its customers when a user interacts with its website, including when an account is created, when a mailing list is joined, a purchase is made, or when a customer engages in an online chat with a customer service representative: Personal identifiers, such as name and address, device and online identifiers and related information, such as telephone number and email address; Internet application, and network activity, demographic information, such as age and date of birth, government identifiers such as national identification numbers and driver's license numbers, financial information such as credit and debit card numbers, purchase history, and geo-location information, among others. *See, e.g.*, https://bonobos.com/privacy, last accessed on April 14, 2021. If a customer makes a purchase through a Bonobos website, its third-party processor service providers may also collect billing information, such as first and last name, email address, phone number, credit card or debit card number, and billing and shipping address. *Id.*

22. The Privacy Policy specifically promises to safeguard class members' Personal Information: "Bonobos has implemented an information security program that includes

administrative, technical and physical controls reasonably *designed to safeguard your personal information*." https://bonobos.com/privacy, last accessed on April 14, 2021.

23. Hackers, however, infiltrated and accessed class members' Private Information in or about August 2020. Threat actors, the Shiny Hunters, stole the class members' Private Information and then posted the stolen information to a hacker website forum. The leaked database included a "70 GB SQL file" containing various internal tables used by the Bonobos website. The database reportedly included customers' addresses, phone numbers, partial credit card numbers (including the last four digits), order information, and password histories, as well as customer email addresses, and IP addresses. On information and belief, the threat actors also turned the cracked passwords into a list used in credential stuffing attacks, which involves utilizing the log in information using the stolen credentials to access other websites.

24. On or about January 22, 2021, Bonobos began emailing breach notifications to affected customers by email, including Plaintiff Cooper.

Plaintiff Cooper's Experience

25. Plaintiff Cooper accessed Defendant Bonobos' website on or about June 28, 2013 and purchased items for approximately $170.00 on his payment card. Mr. Cooper received a confirmation email of his purchase directly from Bonobos. In making this purchase, Mr. Cooper entered his personal identifying information into Defendant's e-commerce payment platform, including his full name, billing and shipping addresses, payment card type and full number, CVV codes, payment card expiration date, email address and telephone number, among other information.

26. Plaintiff Cooper received an email from Defendant Bonobos with the data breach notice on or about January 22, 2021.

27. After receiving notice of the Data Breach, Mr. Cooper changed the password to his

Bonobos account. He also placed a security freeze on his credit through Experian.

28. In addition, Mr. Cooper thereafter purchased credit repair and protection service through Financial Education Services, for which he is paying approximately $85.00 per month. Mr. Cooper also purchased a subscription for the Nomorobo Robocall Blocking application to help block the material number of spam calls that he has been receiving since the Data Breach. He is paying $19.99 for the Nomorobo subscription.

29. As a result of the Data Breach notice, Plaintiff Cooper has spent time dealing with the consequences of the Data Breach, which includes time self-monitoring his accounts, freezing his credit to avoid fraudulent activity, purchasing credit protection service, and purchasing a text spam blocker. In addition, Plaintiff Cooper has spent time dealing with the increased and unwanted spam text, telephone calls, and emails that he continues to receive after the Data Breach.

30. Plaintiff Cooper suffered actual injury in making expenditures which he would not have made had Defendant implemented the necessary and proper safeguards to protect its customers' Private Information from theft.

31. Plaintiff Cooper suffered out of pocket monetary loss, lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has increased concerns for the loss of his privacy.

32. Plaintiff Cooper has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Defendant's Data Security Safeguards Were Inadequate

33. Defendant was on notice of the very real risks of security breaches like the Data Breach. Security breaches like the Data Breach by the Shiny Hunters hacking group have been

frequent and garnered significant media attention over the last decade, with significant data breaches dating back to 2005. The Privacy Rights Clearinghouse, a nonprofit organization which focuses on strengthening privacy protections, has recorded over 9,000 data-related security breaches in the U.S. since 2005, including numerous instances of hacking.[5] Any e-commerce provider – indeed, any business which collects Private Information – is well aware of the risk of security breaches and the need to ensure a robust system of safeguarding against security breaches, whether internally or externally.

34. Plaintiff and other Class members relied on Defendant to implement and maintain systems that kept their Private Information safe. Defendant had a duty to keep its customers' Private Information safe. Defendant failed to comply with this duty.

Password Breaches are Particularly Damaging.

35. Online passwords are the keys to our most sensitive personal information.

36. People typically use the same passwords across all of their websites and applications.[6] "If a password (even a random or complex one) was exposed in a data breach, it can be used by attackers to try the same password on any other website that you use. It can also be used in a 'dictionary' attack with other users."[7]

37. The exposure of a password will also allow hackers to exploit different, but similar, passwords. As one security expert stated, "[o]nce an attacker has access to several users' password formulas, they can easily use cracking rules. This is an attack to create wordlists that will attempt to guess a user's password based on previously used passwords."[8] Similarly, a recent whitepaper

[5] *Data Breaches*, Privacy Rights Clearinghouse, https://privacyrights.org/data-breaches (last visited April 14, 2021).
[6] *See* https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE3y9UJ (last visited April 14, 2021); *see also* https://www.forbes.com/sites/brookecrothers/2020/12/12/how-worried-should-i-be-about-my-password-being-compromised-stolen-in-a-data-breach-experts-say-this/?sh=b421c407468f (last visited April 14, 2021).
[7] https://www.forbes.com/sites/brookecrothers/2020/12/12/how-worried-should-i-be-about-my-password-being-compromised-stolen-in-a-data-breach-experts-say-this/?sh=b421c407468f (last visited April 14, 2021).
[8] *Id.*

sponsored by Microsoft states that "[d]epending on how…users create their passwords…the threat actor still may be able to review user password history and figure out any patterns the user may employ. This technique may allow them to predict the next password in line."[9]

38. Thus, when a password is exposed in a data breach, victims are at imminent risk of further exposure of sensitive data relating to more than just the account that was originally breached.

39. Together, stolen passwords and email addresses, such as what was exposed in the Bonobos data breach, are enough to bypass two-factor authentication ("2FA") and multi-factor authentication ("MFA") protocols (collectively, "2FA/MFA").

40. 2FA/MFA involves "the use of a variety of methods to confirm a user's identity instead of only using a username and password. Often this type of authentication uses a secondary token which changes over time to provide a one-time passcode…."[10] With 2FA/MFA procedures enabled, "users are required to provide a secondary form of verification that normally comes in the form of a numerical token that is either sent via SMS or through a dedicated app to be installed on their phone."[11]

41. SMS 2FA/MFA is the oldest and most common form of 2FA/MFA.[12] SMS 2FA/MFA "validates the identity of a user by texting a security code to their mobile device. The user then enters the code into the website or application to which they're authenticating."[13]

42. Because people lose their phones or change their number, "all services that use SMS-based authentication systems must have recovery services where people can reset their account

[9] https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE3y9UJ (last visited April 14, 2021)
[10] https://www.sc.edu/study/colleges_schools/law/centers/cybersecurity/_docs/fbi_cyber_pin/2019/fbi_pin-20190917_multi-factor_authentication.pdf (last visited April 14, 2021).
[11] https://www.amnesty.org/en/latest/research/2018/12/when-best-practice-is-not-good-enough/ (last visited April 14, 2021).
[12] *See id.*; *see also* https://duo.com/product/multi-factor-authentication-mfa/two-factor-authentication-2fa (last visited April 14, 2021).
[13] https://duo.com/product/multi-factor-authentication-mfa/two-factor-authentication-2fa (last visited April 14, 2021).

or update their phone number. If the attacker has already compromised the email account (perhaps because of re-used passwords), they can reset, update, or otherwise bypass the 2FA system. Lost phone and password-reset pages are the most common targets of unwanted automation today."[14]

43. Victims must also spend copious amounts of time changing their passwords and usernames.[15] Given the propensity of individuals to use the same or similar passwords in multiple accounts, victims must change password and account information for more than just the accounts utilizing the actual username and password data exposed in the breach.

44. When the same or similar passwords are used with financial accounts, or when the data breach includes financial information such as credit card numbers, victims of data breaches must also spend time reviewing all credit and financial history.[16]

The Exposure of Phone Numbers and Email Addresses is Also Very Damaging

45. The exposure of telephone numbers and/or email addresses in a data breach is also very damaging. When the exposure of a telephone number and/or email address is coupled with other data, such as the data exposed in the Bonobos data breach, threat actors receive the tools necessary to conduct malicious phishing attempts and/or bypass 2FA and MFA protocols. Such attacks are often conducted via a form of "social engineering," which exploits common human tendencies resulting from fear and/or trust.

46. A common example of social engineering is where "the attacker calls you, the victim, on your phone, and claims to be a representative of your bank. He says they are checking accounts for fraud, and he is going to send you a code to verify your identity. He asks you to read it back to him, then logs into a site with your credentials while you wait. The 2FA code is sent to you,

[14] https://www.securityweek.com/6-ways-attackers-are-still-bypassing-sms-2-factor-authentication (last visited April 14, 2021).
[15] *See* https://www.consumer.ftc.gov/blog/2016/06/password-breaches-what-do (last visited April 14, 2021).
[16] *See id.*

and you give it to him over the phone. He thanks for you for your help, then robs you of your money and residual dignity."[17]

47. Similarly, threat actors may send fraudulent text messages or emails purporting to be a bank or other service to cause a user to log into a fake website and give up their private information.[18]

48. Through social engineering, a victim's phone number, coupled with other basic information such as the victim's name, is also used to conduct a common form of attack known as "porting" or "SIM swapping." This is where a threat actor takes a victims existing cell-phone number and transfers it to a fake account controlled by the threat actor. Once this has been accomplished, the threat actor can use the victim's phone number to access banking, retirement, health, and other sensitive accounts to commit unlawful and damaging acts such as fraud, theft, and/or the invasion of privacy.[19]

49. The transfer of a victim's phone number to an account controlled by the threat actor is typically accomplished through social engineering techniques involving the victim's phone service provider. A study by Princeton University recently demonstrated how easy it is for a threat actor to successfully perform these attacks with as a little as a victim's name and phone number.[20]

50. In that study, the researchers set up 50 different cell phone accounts across five major phone service providers—AT&T, T-Mobile, Tracfone, US Mobile, and Verizon Wireless (10 accounts with each carrier).[21] The researchers then attempted to conduct "SIM swapping" attacks on each of the accounts. In these fake attacks, the attackers knew only "the victim's name and phone

[17] https://www.securityweek.com/6-ways-attackers-are-still-bypassing-sms-2-factor-authentication (last visited April 14, 2021).
[18] https://www.sc.edu/study/colleges_schools/law/centers/cybersecurity/_docs/fbi_cyber_pin/2019/fbi_pin-20190917_multi-factor_authentication.pdf (last visited April 14, 2021).
[19] *See* https://www.consumerreports.org/scams-fraud/cell-phone-account-fraud/ (last visited April 14, 2021).
[20] *See* https://www.usenix.org/system/files/soups2020-lee.pdf (last visited April 14, 2021).
[21] *Id.*

number. [The researchers] also assumed that the attacker was capable of interacting with the carrier only through its ordinary customer service and account refill interfaces, and for purposes of one attack, that the attacker could bait the victim into making telephone calls to a chosen number."[22]

51. The researchers observed that when they called the customer service departments of these service providers and attempted to switch the phone numbers to new accounts, they were prompted to authenticate their account by providing one or more of the following types of information: the account holder's street address, email address, date of birth, last 4 digits of payment card number, activation date, last payment date and amount, device serial number, SIM serial number, recent numbers called (call log), PIN or password, answers to security questions, SMS one-time passcode, and/or email one-time passcode.[23] Typically, when the researchers gave incorrect authentication information or claimed to not know the information, the customer service representative would simply move on to request a different type of authentication information.[24] Thus, the researchers demonstrated that a threat actor would often be able to switch a victim's phone number to a fake account using nothing more than the type of information contained in the Bonobos Data Breach.

52. Even more troubling, in 8% of the fake attack attempts, the customer service representative allowed the fake attacker to authenticate access to the account with nothing more than the account holder's name, phone number, and knowledge of the account holder's most recent *incoming* calls.

53. Once the victim's number has been ported to a new account, the consequences are nearly certain—and often devastating. From that point on, the threat actor would have complete control of the account. For example, when a financial institution "text[s] a verification code to the

[22] *Id.*
[23] *Id.*
[24] *See id.*

phone number associated with the account—what's known as two-factor identification—that code is sent to the criminal's device, not yours."

54. In a specific example recently highlighted by the FBI, a threat actor was able to port the phone numbers of data breach victims. "Once the attacker had control over the customers' phone numbers, he called the bank to request a wire transfer from the victims' accounts to another account he owned. The bank, recognizing the phone number as belonging to the customer, did not ask for full security questions but requested a one-time code sent to the phone number from which he was calling. He also requested to change PINs and passwords and was able to attach victims' credit card numbers to a mobile payment application."[25]

55. The fact that Plaintiff's and Class members' Private Information was stolen, likely in order to be sold on the dark web and/or used for fraudulent transactions, demonstrates the monetary value of the Private Information.

56. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[26]

Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 billion per year online advertising industry in the United States.[27]

---

[25] https://www.sc.edu/study/colleges_schools/law/centers/cybersecurity/_docs/fbi_cyber_pin/2019/fbi_pin-20190917_multi-factor_authentication.pdf (last visited April 14, 2021).

[26] Tr. at 8:2-8, Federal Trade Commission, *Public Workshop: The Information Marketplace: Merging and Exchanging Consumer Data* (Mar. 13, 2001), https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace- merging-and-exchanging-consumer-data/transcript.pdf (last visited April 14, 2021).

[27] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, The Wall Street Journal (Feb. 28, 2011), http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html (last visited April 14, 2021).

57. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[28]

58. Recognizing the high value that consumers place on their Private Information, many companies now offer consumers an opportunity to sell this information.[29] The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their Private Information. This business has created a new market for the sale and purchase of this valuable data.

59. Consumers place a high value not only on their Private Information, but also on the privacy of that data. Researchers have begun to shed light on how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349.[30]

60. The value of Plaintiff's and Class members' Private Information on the black market is substantial, ranging from $1.50 to $90 per card number.[31]

61. Despite being aware of the value criminals attach to such Private Information,

---

[28] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf (last visited April 14, 2020).
[29] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, The Wall Street Journal (Feb. 28, 2011), http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html (last visited April 14, 2021).
[30] *See* DOJ, *Victims of Identity Theft, 2014* at 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited April 14, 2021), at 6.
[31] Leapfrog, *The Cyber Black Market: What's Your Bank Login Worth* (Mar. 1, 2011), https://leapfrogservices.com/the-cyber-black-market-whats-your-bank-login-worth/ (last visited April 14, 2021).

Defendant failed to ensure its customers were protected from the theft of their Private Information.

62. At all relevant times, Defendant was well-aware, or reasonably should have been aware, that the Private Information it maintains is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft, fraud, and invasion of privacy.

63. Had Defendant remedied the deficiencies in its e-Commerce systems, adequately monitored its e-commerce systems for malicious codes, followed PCI DSS guidelines and, in general, taken reasonable care to prevent and detect security breaches, the Data Breach would have been prevented.

64. Given these facts, any company that transacts business with consumers – who expect their Private Information to be properly safeguarded - and then compromises the privacy of consumers' Private Information has thus deprived consumers of the full monetary value of their transaction with the company.

Damages Sustained by Plaintiff and Class Members

65. A portion of the services purchased from Defendant by Plaintiff and the other Class members necessarily included compliance with industry-standard measures with respect to the collection and safeguarding of Private Information, including their credit and debit card information. The cost to Defendant of collecting and safeguarding Private Information is built into the price of all its services. Because Plaintiff and the other Class members were denied privacy protections that were promised, they paid for, and were entitled to receive, Plaintiff and the other Class members incurred actual monetary damages in that they overpaid for the purchases they made through websites operated by Defendant.

66. Plaintiff and the other members of the Class have suffered additional injury and damages, including, but not limited to one or more of the following:

a. unauthorized use of their Private Information;

b. damages arising from the inability to use their Private Information;

c. monetary costs associated with their attempts to ameliorate, mitigate and deal with the actual and future consequences of the breach, including the freezing of their credit, purchasing and/or supplementation of credit or identity monitoring services, and purchasing of technology designed to block unwanted spam texts, telephone calls, and emails resulting from the Data Breach;

d. time spent and monetary and other costs associated with the loss of productivity or the enjoyment of one's life from taking time to address an attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach (which time spent on those activities Plaintiff and Class members could have been working and earning a living, therefore suffering further actual injury);

e. the imminent and impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;

f. damages to and diminution in value of their Private Information entrusted to Defendant for the sole purpose of purchasing products and services from websites operated by Defendant; and

g. the loss of Plaintiff's and Class members' privacy.

V. CLASS ACTION ALLEGATIONS

67. Plaintiff brings all counts, as set forth below, on behalf of himself and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure, on behalf of a nationwide Class defined as:

All residents of the United States of America whose Private Information was compromised in the Data Breach and who made purchases from Defendant

prior to June 2018 (the "Class").

68. Excluded from the Class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

69. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

70. **Numerosity—Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that joinder of all Class members would be impracticable. On information and belief, Class members number in the tens if not hundreds of thousands.

71. **Commonality and Predominance—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all Class members and predominate over questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. Whether Defendant failed to use reasonable care and commercially reasonable methods to secure and safeguard Plaintiff's and Class members' Private Information;

b. Whether Defendant properly implemented its purported security measures to protect Plaintiff's and Class members' Private Information from unauthorized capture, dissemination, and misuse;

c. Whether Defendant took reasonable measures to determine the extent of the Data Breach after it first learned of same;

d. Whether Defendant disclosed Plaintiff's and Class members' Private Information in violation of the understanding that the Private Information was being disclosed in

confidence and should be maintained;

e. Whether Defendant failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and Class members' Private Information;

f. Whether Defendant was negligent in failing to properly secure and protect Plaintiff's and Class members' Private Information; and

g. Whether Plaintiff and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

72. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of himself and other Class members. Similar or identical common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that predominate in this action.

73. **Typicality—Federal Rule of Civil Procedure 23(a)(3).** Plaintiff's claims are typical of the claims of the other Class members because, among other things, all Class members were similarly injured through Defendant's uniform misconduct described above and were thus all subject to the Data Breach alleged herein. Further, there are no defenses available to Defendant that are unique to Plaintiff.

74. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiff is an adequate Class representative because his interests do not conflict with the interests of the other Class members he seeks to represent, he has retained counsel competent and experienced in complex class action litigation, and Plaintiff will prosecute this action vigorously. The Class' interests will be fairly and adequately protected by Plaintiff and his counsel.

75. **Injunctive Relief-Federal Rule of Civil Procedure 23(b)(2).** Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23(b)(2).

76. **Superiority—Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and the other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for Class members to individually seek redress for Defendant's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

VI. CAUSES OF ACTION

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

77. Plaintiff, individually and on behalf of the Class, repeats and re-alleges the allegations contained in paragraphs 1 through 76 as though fully set forth herein.

78. By virtue of its express undertaking to protect class members' personal information and pon accepting and storing Plaintiff's and Class members' Private Information, Defendant undertook and owed a duty to Plaintiff and Class members to exercise reasonable care to secure and

safeguard that information and to use commercially reasonable methods to do so. Defendant knew that the Private Information was confidential and should be protected as private and confidential.

79. Defendant owed a duty of care not to subject Plaintiff's and Class members' Private Information to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

80. Defendant owed numerous duties to Plaintiff and Class members, including the following:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Private Information;

b. to protect Private Information using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches on its own systems and those of its third parties.

81. Defendant failed to provide adequate supervision and oversight of the Private Information with which it was, and is, entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a malicious third party to gather Plaintiff's and Class members' Private Information, misuse the Private Information and intentionally disclose it to others without consent.

82. Defendant knew, or should have known, of the risks inherent in collecting and storing Private Information, the vulnerabilities of its data collection and/or storage systems, and the importance of adequate security.

83. Defendant knew, or should have known, that its data collection and/or storage systems and networks, including its third-party affiliates, did not adequately safeguard Plaintiff's and Class members' Private Information.

84. Defendant breached its duties to Plaintiff and Class members by failing to ensure that its agents and affiliates were providing fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' Private Information.

85. Because Defendant knew that a breach of its systems would damage an untold number of its customers, including Plaintiff and Class members, Defendant had a duty to adequately safeguard its data systems and the Private Information contained thereon.

86. Defendant had a special relationship with Plaintiff and Class members. Plaintiff's and Class members' willingness to entrust Defendant with their Private Information was predicated on the understanding that Defendant would take adequate security precautions. Moreover, only Defendant had the ability to protect its systems and those of its affiliates, and the Private Information it stored on them, from attack.

87. Defendant also had independent duties under state and federal laws that required it to reasonably safeguard Plaintiff's and Class members' Private Information and promptly notify them about the Data Breach.

88. Through Defendant's acts and omissions described in this Amended Complaint, including its failure to provide adequate security and its failure to protect Plaintiff's and Class members' Private Information from being foreseeably captured, accessed, disseminated, stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiff's and Class members' Private Information during the time it was within Defendant's possession or within its control or in the possession of its agent.

89. The law further imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of the Private Information to Plaintiff and the Class members so that they can take appropriate measures to mitigate damages, protect against adverse consequences, and

thwart future misuse of their Private Information. Defendant failed to do so, only disclosing the Data Breach five months after it occurred.

90. Upon information and belief, Defendant improperly and inadequately safeguarded Plaintiff's and Class members' Private Information in deviation of standard industry rules, regulations, and practices at the time of the unauthorized access. Defendant's failure to take proper security measures to protect Plaintiff's and Class members' sensitive Private Information, as described in this Amended Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of the Private Information.

91. Upon information and belief, neither Plaintiff nor the other Class members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Amended Complaint.

92. As a direct and proximate cause of Defendant's conduct, Plaintiff and Class members have suffered and will suffer damages and injury, including but not limited to:

a. unauthorized use of their Private Information;

b. theft of their Private Information;

c. monetary costs associated with the detection and prevention of spam texts and phone calls and spam emails and identity theft and unauthorized use of their Private Information;

d. damages arising from the inability to use their Private Information;

e. time spent and monetary and other costs associated with the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data

Breach (which time spent on those activities Plaintiff and Class members could have been working and earning a living, therefore suffering further actual injury);

f. the imminent and impending injury flowing from spam texts and phone calls and spam emails posed by their Private Information being placed in the hands of criminals;

g. damages to and diminution in value of their Private Information entrusted to Defendant for the sole purpose of purchasing products and services from website operated by Defendant; and

h. the loss of Plaintiff's and Class members' privacy.

93. As a direct and proximate cause of Defendant's negligence, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to anxiety, emotional distress, loss of privacy, and other economic and non- economic losses.

COUNT II
Violations of New York Consumer Law for Deceptive Acts and Practices
N.Y. Gen. Bus. Law § 349
(On Behalf of Plaintiff and the Class)

94. Plaintiff, individually and on behalf of the Class, repeats and re-alleges the allegations contained in paragraphs 1 through 76 as though fully set forth herein.

95. New York General Business Law ("NYGBL") § 349 prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of New York.

96. The law of the State of New York applies to all customer disputes with respect to customer purchases from Defendant's e-commerce websites. Plaintiff made his purchases in the State of New York. Bonobos has its headquarters in the State of New York.

97. By reason of the conduct alleged herein, Defendant engaged in unlawful practices within the meaning of the NYGBL § 349. The conduct alleged herein is a "business practice" within the meaning of the NYGBL § 349, and the deception occurred in part within New York State.

98. Defendant stored Plaintiff's and the Class members' Private Information in Defendant's electronic and consumer information databases. Defendant knew or should have known that it did not employ reasonable, industry standard, and appropriate security measures that complied "with federal regulations" and that would have kept Plaintiff's and the Class members' Private Information secure and prevented the loss or misuse of Plaintiff's and the Class members' Private Information.

99. Defendant did not disclose to Plaintiff and the Class members that its data systems were not secure. To the contrary, Defendant expressly represented on its website that it would safeguard its customers' personal information.

100. Plaintiff and the Class members never would have provided their sensitive and Private Information if they had been told or knew that Defendant and its affiliates failed to maintain sufficient security to keep such Private Information from being hacked and taken by others, and that Defendant failed to maintain the information in a properly encrypted form.

101. Defendant violated the NYGBL §349 by failing to properly represent, both by affirmative conduct and by omission, the safety of Defendant's many systems and services, specifically the security thereof, and their ability to safely store Plaintiff's and the Class members' Private Information.

102. Defendant also violated NYGBL §349 by failing to implement reasonable and appropriate security measures or adequately follow industry standards for data security, and by failing to immediately notify Plaintiff and the Class members of the Data Breach. If Defendant had

complied with these legal requirements, Plaintiff and the other Class members would not have suffered the extent of damages caused by the Data Breach.

103. Defendant's practices, acts, policies and course of conduct violate NYGBL § 349 in that:

a. Defendant actively and knowingly misrepresented or omitted disclosure of material information to Plaintiff and the Class members at the time they provided such Private Information that Defendant did not have sufficient security or mechanisms to protect Private Information;

b. Defendant failed to give timely warnings and notices regarding the defects and problems with its system(s) of security (and the security of their affiliates) that it maintained to protect Plaintiff's and the Class members' Private Information;

104. Plaintiff and Class members were entitled to assume, and did in fact expressly assume, Defendant would take appropriate measures to keep their Private Information safe. Defendant did not disclose at any time that Plaintiff's and the Class members' Private Information was vulnerable to hackers.

105. The aforementioned conduct constitutes an unconscionable commercial practice in that Defendant has, by the use of false statements and/or material omissions, failed to properly represent and/or concealed the defective security system that it and its affiliates maintained and failed to reveal the Data Breach timely and adequately.

106. Members of the public were deceived by and relied upon Defendant's affirmative misrepresentations and failures to disclose.

107. Such acts by Defendant are and which are and/or were likely to mislead a reasonable consumer providing his or her Private Information to Defendant. Said acts and practices are material. The requests for and use of such Private Information in New York through such means occurring in

New York were consumer-oriented acts and thereby fall under the New York consumer protection statute, NYGBL § 349.

108. Defendant's wrongful conduct caused Plaintiff and the Class members to suffer a consumer-related injury by causing them to incur actual and future loss of time and expense to protect from misuse of the Private Information materials by third parties and placing the Plaintiff and the Class members at serious risk for monetary damages.

109. As a direct and proximate cause of Defendant's conduct, Plaintiff and Class members suffered damages as alleged above.

110. In addition to or in lieu of actual damages, because of the injury, Plaintiff and the Class members seek statutory damages for each injury and violation which has occurred.

COUNT III
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

111. Plaintiff, individually and on behalf of the Class, repeats and re-alleges the allegations contained in paragraphs 1 through 76 as though fully set forth herein.

112. Plaintiff and Class members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and provided Defendant with their payment information. In exchange, Plaintiff and Class members should have received from Defendant the goods and services that were the subject of the transaction with protection of their Private Information with adequate data security.

113. Defendant knew that Plaintiff and Class members conferred a benefit on it and accepted or retained that benefit. Specifically, Defendant profited from Plaintiff's purchases and

used Plaintiff's and Class members' Private Information for business purposes at the expense of Plaintiff and Class members.

114. Defendant failed to secure Plaintiff's and Class members' Private Information and, therefore, did not provide full compensation for the benefit the Plaintiff's and Class members' Private Information provided.

115. Defendant acquired the Private Information through inequitable means as they failed to adequately safeguard the Private Information of Plaintiff and Class members as promised.

116. If Plaintiff and Class members knew that Defendant would not secure their Private Information using adequate security, they would not have made purchases on Defendant's website.

117. Plaintiff and Class members have no adequate remedy at law.

118. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class members conferred on Defendant.

119. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class members overpaid.

VII. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of all claims so triable.

VIII. REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Class proposed in this Amended Complaint, respectfully requests that the Court enter judgment in his and the Class' favor and against Defendant, as follows:

A. Declaring that this action is a proper class action, certifying the Class as requested herein, designating Plaintiff as Class Representative, and appointing Class Counsel as requested in Plaintiff's expected motion for class certification;

B. Ordering Defendant to pay actual/statutory damages as appropriate to Plaintiff and the other members of the Class;

C. Ordering Defendant to pay punitive damages, as allowable by law, to Plaintiff and the other members of the Class;

D. Ordering Defendant to pay attorneys' fees and litigation costs to Plaintiff and his counsel;

E. Ordering Defendant to pay equitable relief, in the form of disgorgement and restitution, and injunctive relief as may be appropriate;

F. Ordering Defendant to pay both pre- and post-judgment interest on any amounts awarded; and

G. Ordering such other and further relief as may be just and proper.

Date: April 14, 2021.

Respectfully submitted,

/s/ Lori G. Feldman
Lori G. Feldman (LF-3478)
GEORGE GESTEN MCDONALD PLLC
102 Half Moon Bay Drive
Croton-on-Hudson, New York 10520
Phone: (917) 983-9321
Fax: (888) 421-4173
Email: LFeldman@4-Justice.com
E-Service: eService@4-Justice.com

David J. George (*pro hac vice*)
Brittany L. Brown (*pro hac vice*)
GEORGE GESTEN MCDONALD, PLLC
9897 Lake Worth Road, Suite #302
Lake Worth, FL 33467
Phone: (561) 232-6002
Fax: (888) 421-4173
Email: DGeorge@4-Justice.com
BBrown@4-Justice.com
E-Service: eService@4-Justice.com

Terence R. Coates (*pro hac vice*)
Justin C. Walker (*pro hac vice*)
MARKOVITS, STOCK & DEMARCO, LLC
3825 Edwards Road, Suite 650
Cincinnati, OH 45209
Phone: (513) 651-3700
Fax: (513) 665-0219
Email: tcoates@msdlegal.com
jwalker@msdlegal.com

Attorneys for Plaintiff